UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/936,570	12/06/2001	Toru Sorimachi	2565-0236P	8713

2292 7590 04/07/2006

BIRCH STEWART KOLASCH & BIRCH
PO BOX 747
FALLS CHURCH, VA 22040-0747

EXAMINER	
TRAN, ELLEN C	

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 04/07/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/936,570	SORIMACHI ET AL.	
	Examiner	Art Unit	
	Ellen C. Tran	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 December 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-50* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-50* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This action is responsive to communication: amendment filed 30 December 2005 with recognition of a filing date of application filed 06 December 2001 with continuing data of a PCT filed on 22 December 2000 and a foreign application filed on 14 January 2000.

2. Claims 1-50 are currently pending in this application. Claim 1, 5, 7, 8, 10, 11, 15, 17, 18, 20, 21, 23, 24, 26, 27, 29, 30, 31, 32, 45, 46, 47, and 48 are independent claims, claims 1-5, 7, 8, 10-15, 17, 18, 20, 21, 23, 24, 26, 27, 29, 30, and 32 have been amended. Amendments to the claims and the specification have been accepted.

3. Note applicant indicates that drawings are amended but no replacement sheet is visible in the scanned images.

Response to Arguments

4. Applicant's arguments with respect to claims 1-50 have been considered but they are not found persuasive.

With respect to applicant's argument on page 31, "Accordingly, none of Markham's encrypting processes encrypts a logically continuous set of data elements, such as successive set of plain text data blocks (M1, N2, N3, ...)". The Office disagrees Markham does teach encrypting a logically continuous set of data elements the keystream is decoupled as indicated by col. 6, lines 41-44, however the process still encrypts the next available element. The decoupling just as in the claimed invention removes the dependence on the first data element to be encrypted before the second element starts the encryption process.

With respect to applicant's argument on page 31, "Also because Markham similarly discloses decoupling the decryption of one cipher block from the next cipher block, each

decrypting process in Markham fails to produce a continuous set of data elements (e.g. plain text blocks)". The Office disagree Markham discloses decrypting elements in order FIFO as shown in col. 6, lines 41-44, the decoupling is just another term that has the same meaning as the applicant's invention.

With respect to applicant's arguments beginning on page 31 with respect to independent claims 1, 5, 7, 11, 15, 17, 21, 23, 27, and 29 "comprises a first logically continuous set of data elements" and 'encrypting or decryting the next element before completing the previous'. The Office disagrees as stated above the decoupling does not change that the keystream is continuously encrypted or decrypted. Like the claimed invention the second data element can begin the encryption or decryption process before the previous element has completed.

With respect to applicant's argument on page 32, "Accordingly, Applicants respectfully submit that Jakubowski fails to disclose a MAC generating unit or method, which inputs encrypted/decrypted data output from an encrypting/decrypting unit. Instead Jakubowski expressly teaches that the MAC is generated from the intermediate stream. During encryption, this intermediate stream is produced before encrypted data (ciphertext) is output from the encrypting unit/step. Likewise, during decryption the intermediate stream is recovered before plaintext data is output from the decrypting unit/step". The Office disagrees with argument and notes that Jakubowski teaches the claimed invention, an 'intermediate stream' which is produces during encryption or decryption has the same meaning as the claimed text 'wherein the MAC generator starts generating the MAC before completion of encrypting the data by the encrypting unit".

With respect to applicant's arguments beginning on page 33, "However, according to Fig. 4A and col. 9, lines 6-16 ... Jakubowki's MAC is defined as a predetermined portion of the intermediate stream Y0...Yn, which is encrypted and inserted into the output ciphertext Co..Cn. Thus, as shown in Fig. 4A, Jakuboweski fails to teach that a ciphertext block Ci is used an input for generating the MAC, as required by claims 8, 10, 18, 20, 24, 26, 30, and 32". The Office disagree with argument and notes the applicant interpretation of Fig. 4A is the opposite of what is shown. The Fig shows the encryption process, the first input to the encryption process is the plaintext, the next step inserts the MAC into the encryption process.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language

6. **Claims 1-7, 11-17, 21-23, 27-29, 33, 35, 37, 39, and 41-44,** are rejected under 35 U.S.C. 102(e) as being anticipated by Markham U.S. Patent No. 5,796,836 (hereinafter '836).

As to independent claim 21, "An encrypting apparatus encrypting plaintext data M including plaintext block data M, (i = 1, 2, 3, ...) and plaintext data N including plaintext,

block data N, (j = 1, 2, 3, ...), the encrypting apparatus comprising:" is taught in '836 col. 3, lines 35-67;

"a mechanism for receiving a request to encrypt the plaintext data N1 during encrypting process of the plaintext data M before completion of the encrypting process of the plaintext data M" is shown in '836 col. 7, lines 21-29;

"an encrypting module for outputting encrypted data as module output block data T_1" is disclosed in '836 col. 7, lines 7-12;

"a feedback loop for feeding back the module output block data T, output from the encrypting module to the encrypting module through a feedback line" is taught in '836 col. 7, lines 13-20;

"a memory, provided in parallel with the feedback line of the feedback loop fur receiving the request to encrypt, the plaintext data N, and storing the module output block data T, fed back when the plaintext block data M_i is not encrypted subsequent to the plaintext block data M_i so that an encrypting process of any plaintext block data of the plaintext data N is started; and" is shown in '836 col. 8, lines 14-67;

"a selector for selecting and supplying the module output block data T_i, fed back through the feedback line of the feed back loop to the feedback loop in case that the plaintext block data M_{i+1}, is encrypted subsequent to the plaintext block data T_i and for selecting and supplying the module output block T_i, stored in the memory to the feedback loop in case that the plaintext block data M_{i+1} is not encrypted subsequent to the plaintext block data M_i and the plaintext block data M_{i+1} is encrypted after any of plaintext block data of the plaintext data N is encrypted" is disclosed in '836 col. 12, lines 1-67;

"wherein the plaintext block data Mi (i=1,2,3,...) are logically continuous data elements, and the plaintext block data nj(j=1,2,3,...) are logically continuous data elements" is taught in '836 col. 4, lines 21-26 .

As to dependent claim 22, "wherein the memory includes: plural registers corresponding to plural pieces *of* plaintext data" is taught in '836 col. 13, lines 1-8;

"and a switch switching registers corresponding to the plaintext data to be encrypted" is shown in '836 col. 8, lines 17-58.

As to independent claim 5, this claim contains substantially similar subject matter as independent claim 21; therefore it is rejected along the same rationale.

As to dependent claim 6, this claim contains substantially similar subject matter as claim 22; therefore it is rejected along the same rationale.

As to independent claim 23, "An encrypting method comprising the steps of: encrypting plaintext block data M_i (i = 1, 2, 3, ...) of first plaintext data M using ciphertext block data T_i (i = 1, 2, 3, ...) output from an encrypting module" is taught in '836 col. 7, lines 13-20;

"storing ciphertext block data T_i to be used for encrypting plaintext block data M_{i+1} of the first plaintext data M in a memory during or after encrypting process; of the plaintext block data M_i" is shown in '836 col. 8, lines 14-67;

"encrypting at least one plaintext block data of second plaintext data N after storing the ciphertext block data T_i to be used for encrypting the plaintext block data M_{i+1} in the memory" is disclosed in '836 col. 12, lines 1-67;

"and inputting the module output block data T_i to be used for encrypting the plaintext block data M_{i+1} stored in the memory after encrypting the at least one plaintext block data of the second plaintext data N and encrypting the plaintext block data M_i of the first plaintext data M using the encrypting module" is taught in '836 col. 7, lines 21-38

"wherein the plaintext block data Mi (I=1,2,3,...) are logically continuous data elements, and the plsintext block data nj(j=1,2,3,...) are logically continuous data elements" is taught in '836 col. 4, lines 21-26 .

As to independent claim 7, this claim contains substantially similar subject matter as independent claim 23; therefore it is rejected along the same rationale.

As to independent claim 1, "An encrypting apparatus encrypting first processing data and second processing data comprising: a memory for storing a status of an encrypting process" is taught in '836 col. 3, lines 35-67;

"wherein the encrypting apparatus starts encrypting process of the second processing *data* before an encrypting process of *the first* processing data is completed, the encrypting apparatus causes the memory to store the status of the encrypting process of the first processing data when the encrypting apparatus starts the encrypting process of the second processing data, the encrypting of the encrypting process of the encrypting apparatus is returned to the status of the encrypting process of the first processing data stored in tile memory when the encrypting apparatus restarts encrypting the first processing data, and the first processing data" is shown in '836 col. 7, lines 13-37;

"comprises a first logically continuous set of data elements, and the second processing data comprises a second logically continuous set of data elements" is taught in '836 col. 4, lines 21-26 .

As to dependent claim 2, "wherein the encrypting apparatus restarts the encrypting process of the first processing data before the encrypting process of the second processing data is completed, the memory stores the status of the encrypting process of the second processing data when the encrypting apparatus *restarts the* encrypting process of the first processing data, the encrypting of the encrypting *apparatus is returned* to the status of the encrypting process of the second processing data stored in the memory when the encrypting apparatus restarts encrypting process of the second processing data" is disclosed in '836 col. 12, lines 1-67.

As to dependent claim 3, "wherein the first processing data is a continuous set of plaintext data blocks and the second processing data is another plaintext data" is taught in '836 col. 7, lines 21-37.

As to dependent claim 4, "the encrypting apparatus starts encrypting process of the second processing data in response to receiving an interrupt" is shown in '836, col. 12, line 59 through col. 13, line 9.

As to dependent claim 41, "wherein the encrypting process is performed using block cipher algorithm" is disclosed in '836 col. 5, lines 25-35.

As to dependent claim 43, "wherein the memory stores an intermediate encrypting result of the first processing data and an encryption key to be used for encrypting the first

processing data as the status of the encrypting process" is taught in ''836, col. 12, line 59 through col. 13, line 9.

As to independent claim 11, "A decrypting apparatus decrypting first processing data and second processing data comprising a memory for storing a status of a decrypting process" is taught in '836 col. 3, lines 35-67 and '836 col. 9, lines 30-33;

"wherein the decrypting apparatus starts the decrypting process of the second processing data before the decrypting process of the first processing data is completed, the decrypting apparatus causes the memory store the status of the decrypting process of the first processing data when the decrypting process of the second processing data is started, and the decrypting status of the decrypting apparatus is returned to the status of the decrypting process of the first processing data stored in the memory when the decrypting process of the first processing data is restarted, and the first processing data" is shown in '836 col. 7, lines 13-37;

"comprises a first logically continuous set of data elements, and the second processing data comprises a second logically continuous set of data elements" is disclosed in '836 col. 4, lines 21-26 .

As to dependent claims 12-14, 42, and 44, these claims contain substantially similar subject matter as claims 2-4, 41, and 43; therefore they are rejected along similar rationale.

As to independent claim 15, "A decrypting apparatus decrypting ciphertext block data C, (i = 1, 2, 3, ...) included in ciphertext data C and ciphertext block data D_j (j = 1, 2, 3, ...) included in ciphertext data D, the decrypting apparatus comprising" is taught in '836 col. 3, lines 35-67 and col. 9, lines 30-33;

"a mechanism for receiving a request to decrypt the ciphertext data D at an arbitrary timing during a decrypting process of the ciphertext data C; is shown in '836 col. 7, lines 21-29;

"a decrypting unit for performing the decrypting process of the ciphertext block data C, to output plaintext block data M_i" is disclosed in '836 col. 7, lines 7-12;

"a feedback loop for feeding back the ciphertext block data C_i to be used for decrypting ciphertext block data C_{i+1} to the decrypting unit through feedback line" is taught in '836 col. 7, lines 13-20;

"a memory, provided in parallel with the feedback line of the feedback loop, for receiving the request to decrypt the ciphertext data D and storing the ciphertext block data C_i fed back when the ciphertext block data C_{i+1} is not decrypted subsequent to the ciphertext block data C_i so that the decrypting; process of any of ciphertext block data of the ciphertext data D is started; and" is shown in '836 col. 8, lines 14-67;

"a selector for selecting and supplying the ciphertext block data C_i fed back from the feedback line of the feedback loop in case that the ciphertext block data C_{i+1} is decrypted subsequent to the ciphertext block data C_i and for selecting, and ,supplying the ciphertext block data C_i stored in the memory in case that the ciphertext block data C_{i+1} is not decrypted subsequent to the ciphertext block data C_i and the ciphertext block data C_{i+1} is decrypted after any of the ciphertext block data of the ciphertext data D is decrypted" is disclosed in '836 col. 12, lines 1-67;

"wherein the plaintext block data Mi (i=1,2,3,...) are logically continuous data elements, and decryption of the ciphertext data D results in another plaintext data N being output" is taught in '836 col. 4, lines 21-26 .

As to dependent claim 16, this claim is substantially similar to dependent claim 22; therefore it is rejected along the same rationale.

As to independent claim 17, "A decrypting method comprising the steps of: decrypting plaintext block data C_i (i = 1, 2, 3, ...) of first plaintext data C using a decrypting module" is taught in '836 col. 7, lines 13-20 and '836 col. 9, lines 30-33;

"storing ciphertext block data C_i to be used for decrypting plaintext block data C_{i+1} of the first plaintext data M in a memory during or after decrypting process; of the plaintext block data C_i" is shown in '836 col. 8, lines 14-67;

"decrypting at least one plaintext block data of second plaintext data D after storing the ciphertext block data C_i to be used for decrypting the plaintext block data C_{i+1}" is disclosed in '836 col. 12, lines 1-67;

"and inputting the ciphertext block data C_i to be used for decrypting the ciphertext block data C_{i+1} stored in the memory after decrypting the at least one ciphertext block data of the ciphertext block data of the ciphertext data D and decrypting the ciphertext block data C_{i+1} of the first ciphertext data C using the decrypting module" is taught in '836 col. 7, lines 21-38;

"wherein the plaintext block data Mi (i=1,2,3,...) are logically continuous data elements, and decryption of the ciphertext data D results in another plaintext data N being output" is taught in '836 col. 4, lines 21-26 .

As to independent claim 29, "A decrypting method comprising steps of: decrypting ciphertext block data C_i (i = 1, 2, 3, ...) of first ciphertext *data C using module* output block data T_i (i = 1, 2, 3, ...) output from a decrypting module" is taught in '836 col. 7, lines 13-20 and '836 col. 9, lines 30-33;

"storing nodule output block data T_i to be used for decrypting ciphertext block data C_{i+1} of the first ciphertext data G in a memory during or after a decrypting process of the ciphertext block *data* C_i" is shown in '836 col. 8, lines 14-67;

"decrypting, at least one ciphertext block data Djof second ciphertext data D after storing the module output block data T_i to be used for decrypting the ciphertext block data C_{i+1} in the memory; and" is disclosed in '836 col. 12, lines 1-67;

"decrypting the ciphertext block data C_{i+1} of the first ciphertext data C using the decrypting module by inputting the module output. block data T_i to be used for the ciphertext block data C_{i+1} stored in the memory after decrypting the at least one ciphertext block data of the second ciphertext data D" is taught in '836 col. 7, lines 21-38;

"wherein the plaintext block data Mi (i=1,2,3,...) are logically continuous data elements, and decryption of the ciphertext data D results in another plaintext data N being output" is taught in '836 col. 4, lines 21-26 .

As to independent claim 27, this claim is directed to the apparatus of the method of claim 29; therefore it is rejected along the same rationale.

As to dependent claim 28, " wherein the memory includes: plural registers corresponding to plural cipphertext data" is taught in '836 col. 13, lines 1-8;

"and a switch for switching the plural registers corresponding to the ciphertext data to be decrypted" is shown in '836 col. 8, lines 17-58.

As to dependent claims 33, 35, 37, and 39, these claims are directed to a computer readable medium of the previously identified claims; therefore they are rejected along the same rationale.

7. **Claims 45-50,** are rejected under 35 U.S.C. 102(e) as being anticipated by Jakubowski et al. U.S. Patent No. 6,226,742 (hereinafter '742).

As to independent claim 47, "An encrypting method comprising: an encrypting step for inputting data to encrypt and outputting encrypted data" is taught in '742 col. 5, lines 51-65;

"and a MAC generating step for inputting the encrypted data output from the encrypting step and generating a MAC for ensuring an integrity of the encrypted data" is shown in '742 col. 9, lines 34-59;

"and wherein the MAC generating step starts generating the MAC before completion of encrypting the data by the encrypting step" is disclosed in '742 col. 9, lines 4-33.

As to independent claim 48, "A decrypting method comprising: a decrypting step for inputting data to decrypt and outputting decrypted data" is taught in '742 col. 5, line 66 through col. 6, line 13;

"and a MAC generating step for inputting the decrypted data output from the decrypting step and generating a MAC for ensuring an integrity of the encrypted data" is shown in '742 col. 9, lines 34-59;

"and wherein the MAC generating step starts generating the MAC before completion of decrypting the data by the decrypting step" is disclosed in '742 col. 9, lines 4-33.

As to dependent claim 49, "A computer readable storage medium storing a program for having a computer execute steps for the encrypting method described in claim 47" is taught in '742 col. 8, lines 63-67.

As to dependent claim 50, "A computer readable storage medium storing a program for having a computer execute steps for the decrypting method described in claim 48" is shown in '742 col. 8, lines 63-67.

As to independent claim 45, this claim is directed to the apparatus of claim 47; therefore it is rejected along the same rationale.

As to independent claim 46, this claim is directed to the apparatus of claim 48; therefore it is rejected along the same rationale.

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. **Claims 8-10, 18-20, 24-26, 30-32, 34,36,38, and 40** are rejected under 35 U.S.C. 103(a) as being unpatentable over Markham U.S. Patent No. 5,796,836 (hereinafter '836) in further view of Jakubowski et al. U.S. Patent No. 6,226,742 (hereinafter '742).

As to dependent claim 10, "An encrypting method for encrypting plaintext, data including at least one plaintext block data into ciphertext data using an encrypting unit" is taught in '836 col. 3, lines 35-67 "The present invention provides a system and method for decoupling encrypting of one plain text block from the encryption of the next plain text block"

"an encrypting step, including a first feedback step for feeding back ciphertext block data C_i (I-1,2,3,...)output from the encrypting unit when the encrypting unit encrypts plaintext block data, inputting the plaintext block data Mi(i=1,2,3,...), performing an encrypting process by feeding back the ciphertext block data C_i through a first feedback loop, and outputting a ciphertext block data" is shown in '836 col. 7, lines 7-20 "As an example, consider the cipher feedback mode embodiment shown in FIG. 4. The mode shown uses three encncryption device modules 52.1-3. Each encryption device module 52 includes a codebook module 32, an output register 54, and an encryption module";

the following is not taught in '836:

"and generating a message authentication code (MAC) to ensure an integrity of the ciphertext data, the encrypting method comprising:" however '746 teaches "The encrypted MAC is advantageously extended throughout the remainder of the ciphertext message. The encrypted MAC is then inserted into the ciphertext message as block n-1 and n" in col. 9, lines 51-65;

"a MAC generating step, including a second feedback step for feeding back a computed intermediate MAC result, inputting the ciphertext block data whenever the ciphertext block data is output from the encrypting step, processing data" however '746

teaches "Illustratively, two blocks in the intermediate bit stream, i.e., Y_{n-1} and Y_n are concatenated together to form a 54-bit MAC (Y_{n-1}, Y_n) .... By chaining a plaintext message and defining the MAC as a predefined protion, e.g., (Y_{n-1}, Y_n) of the ensuing chained message, the MAC can be generated rather quickly and efficiently" in col. 9, lines 34-59;

"feeding back the computed intermediate MAC result through the second feedback step, and generating the MAC to ensure the integrity of the ciphertext data, wherein the ciphertext block data Ci is input to the MAC generating step before the ciphertext block data Ci+1 is output by the encrypting step" however '742 teaches "Through our present invention, a plaintext message can be securely encrypted and any violations of the integrity of a resulting ciphertext message can readily detected by, during encryption generating, in response to an incoming plaintext message, and intermediate stream, wherein a predefined portion of the intermediate stream defines a message authentication code (MAC)" in col. 9, lines 4-33 as well as Fig. 4A.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of '836, a cipher block chaining mechanism for encryption and decryption to enhance the security of messages exchange. One of ordinary skill in the art would have been motivated to perform such a modifications because of the growth in the Internet and technology (see '742 col. 3, lines 24 et seq.). "Therefore, a need exists in the art for a cryptographic technique that not only provides an extremely high level of security against cryptanalysis, particularly given the sophistication and power of current and future processing technology, but also is capable of detecting a change made to a ciphertext message".

As to independent claim 8, this claim is directed to the apparatus of the method of claim 10; therefore it is rejected along the same rationale.

As to dependent claim 9, "wherein the encrypting unit. and the MAC generator perform alternately the encrypting process and a MAC generating process by sharing one encrypting module and one feedback loop, and wherein the one feedback loop includes a memory for respectively storing and outputting results of the encrypting process and the MAC generating process; and a selector for selecting alternately the results of the encrypting process and the MAC generating process from the memory to alternately perform the encrypting process kind the MAC generating process" is taught in '742 col. 14, lines 1-27 "FIG. 5 depicts a flowchart of Encryption procedure 500. Upon entry to this procedure, block 510 is first executed to calculate the value of a zero-th output block of intermediate stream, Y, as being equal to $F(eP_0)$ and a block counter, i, to the value one. Thereafter, execution enters Encryption--Forward CBC procedure 520 which, given the plaintext as input, computes the intermediate bit stream through a forward cipher block chain. In particular, execution first proceeds to block 525 which determines for block i in the plaintext stream, i.e., P_i, and block i-1 in the intermediate stream, i.e., Y_{i-1}, the value of block i in the intermediate stream, Y_i, depending on whether the value of counter i is then even or odd, through the use of equation (4) or (5) above, respectively. Once the value of block Y_i is so determined, execution proceeds to decision block 530. This decision block determines if all n+1 blocks in the intermediate bit stream have been generated. If any such block remains to be calculated, then decision block 530 routes execution, via NO path 534, to block 535. The latter block increments the block counter by one. Execution then loops back, via path 537, to block 525 to generate the

value of the next block in the intermediate stream, and so forth. Alternatively, if all such blocks have been generated, then decision block 530 routes execution, via YES path 532, out of procedure 520 and to block 540".

As to independent claim 20, "A decrypting method decrypting ciphertext data including at least one ciphertext block data into plaintext data" taught in '836 col. 3, lines 35-67

"and generating a message authentication code (MAC) for ensuring an integrity of the ciphertext data" in col. 9, lines 51-65;

"the decrypting method comprising: a decrypting step including a first feedback step for feeding back module output block data Ti(i=1,2,3,...), generated at decrypting data by a decrypting module, inputting the ciphertext block data Ci(i=1,2,3,...), decrypting the ciphertext block data Ci using the module output block data T, fed back through the first feedback loop, and outputting plaintext block data Ci" is shown in '836 col. 7, lines 7-20

"a MAC generating step including a second feedback step for feeding back a computed intermediate MAC result, inputting ciphertext block data Ci identical to the ciphertext block data input to the decrypting unit, processing the darn, outputting the computed intermediate MAC result" is disclosed in '742 col. 9, lines 34-59;

"feeding back the computed intermediate MAC result by the second feedback loop, and generating the MAC for ensuring the integrity of ciphertext data wherein the ciphertext block data Ci is input to thte MAC generating step before the ciphertext block data Ci+1 is decrypted by the decrypting step" is taught in '742 col. 9, lines 4-33 and Fig. 4A.

As to independent claim 18, this claim is directed to the apparatus of the method of claim 20; therefore it is rejected along the same rationale.

As to dependent claim 19, "wherein the decrypting unit and the MAC generator share one decrypting module and one feedback loop and alternately perform a decrypting process and a MAC generating process, and wherein the one feedback loop includes: a memory storing and outputting results of the decrypting process and the MAC generating process; and a selector for alternately selecting the results of the decrypting process and the MAC generating process to output to the decrypting module for alternately performing the decrypting process and the MAC generating process" is taught in '742 col. 15, lines 15-42 "FIGS. 7A and 7B collectively depict a flowchart of Decryption procedure 700; the correct alignment of the drawing sheets for these figures is shown in FIG. 7. Upon entry to this procedure, block 705 is first executed to decrypt the encrypted MAC, i.e., ($\mathbf{Y_{n-1}}$', $\mathbf{Y_n}$'), residing in the two highest-order blocks, i.e., $\mathbf{C_{n-1}}$ **and** $\mathbf{C_n}$, of incoming ciphertext message C. The decryption algorithm used is an inverse pseudo-random permutation of that which created the encrypted MAC".

As to independent claim 24, this claim is directed to the apparatus of the method of claim 10; therefore it is rejected along similar rationale.

As to dependent claim 25, this claim contains substantially similar subject matter as claim 9; therefore it is rejected along the same rationale.

As to independent claim 26, this claim contains substantially similar subject matter as claim 10; therefore it is rejected along the same rationale.

As to independent claim 30, this claim is directed to the apparatus of the method of claim 20; therefore it is rejected along similar rationale.

As to dependent claim 31, this claim contains substantially similar subject matter as claim 19; therefore it is rejected along the same rationale.

As to independent claim 32, this claim contains substantially similar subject matter as claim 20; therefore it is rejected along the same rationale.

As to dependent claims 34, 36, 37, and 40, these claims are directed to a computer readable medium of the previously identified claims; therefore they are rejected along the same rationale.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a). A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ellen C Tran whose telephone number is (571) 272-3842. The examiner can normally be reached from 6:00 am to 2:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jacques H. Louis-Jacques can be reached on (571) 272-6962. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

ECT

Ellen Tran
Patent Examiner
Technology Center 2134
1 April 2006